The politics of Cyber Security policy making in Africa: The Case Study of Uganda

Owiny, Moses (2019)

Key Words: Cyber Security | Security| Cyber Laws| Africa

Abstract:

African countries enacted several cyber security laws to deal with insecurities in network infrastructures and computers as a way of mitigating cyber-attacks caused by malware intrusion, hackers, criminal fraudsters, extremists' groups, cyber espionage actors among others. This paper argues that cyber threats are often shrouded in a cloud of speculative semantics worsened by the ambiguity in definitions of security issues with terminologies that raises alarm and dramatizes security issues. The article examines the discursive constructions of security issues within the context of three major cyber security threat framing i.e. the technical, crime-espionage and civil defense discourse to inform the arguments that Security issues in Africa has been highly politicized based on fears, risks and assumptions outside the normal realities of an existential threat.

1.0 Introduction

The internet technology that we use today is one of the significant technology developments that happened to the globe. The internet research design started in 1973 and the network became operational in 1983. By early 1990's the technology began proliferating into the mainstream society and its now widely regarded as a general purpose technology without which the modern society couldn't function (Naughton, 2016) . The internet revolution present opportunities such as increased commerce, faster flow of communication and networking, increased inter dependence and globalization amongst others. The same internet also presents challenges for instance, cyber-crime – manifesting through attacks and damage to critical network infrastructures, malicious malware intrusions, state sponsored attacks including cyber espionage amongst others. In fact, cyber security as a framework evolved as one of the most significant concerns of the global North and Africa since the concept first gained prominence in the western discourse in the early 1990s.

Cyber Security accounts for technologies, processes as well as practices, designed to protect networks and various computer programs as well as data from attack, damage and unauthorized access (Cabinet, 2011). The insecurities reflect threats and attacks on critical national infrastructures including other forms of organized cyber-attacks that takes forms such as hacktivism, basic malware intrusions as well as internal misuse of systems and software malfunctions (Creasey, 2013) . Cyber-attack may also take forms of serious organized criminals, state sponsored attacks or extremist elements and these often targets critical infrastructures such as power plants and facilities, water, transportation and communication systems often launched via cyber space.

Security as a concept has arguably been a contested concept with no universally agreed definition. (Baldwin, 1997) notes that the concept of security is quite ambiguous to the extent when used without any specification. He argues that any definition of security must articulate the referent object that are threatened – security for whom and notes that security is so value laden. Understanding how much security and for what threats is very important in defining security and providing prescriptions to insecurities.

The conceptual understanding of security is crucial in cyber security as a framework as the same interpretive logic of security with specifications as articulated by (Baldwin, 1997) applies. In cyber security policy making, policy makers must be able to identify security threats, the referent objects under threat, and what amount of security is required with high degree of specification otherwise, labeling something just as a threat in the cyber space would be ambiguous. Cyber Space refers to an interactive domain consisting of digital networks that is used to store, modify and communicate information and includes the internet as well as other information systems (Cabinet, 2011) . It then follows that Cyber Security accounts for technologies, processes as well as practices, designed to protect networks and various computer programs as well as data from attack, damage and unauthorized access (Thierry Balzacq, 2016).

It is however, important to note that having a strong conceptual understanding of security as a concept provides a better analysis of insecurities in the cyber space. It is also important to make an argument as to whether cyber security is any different from the concept of old wars and insecurity or if it falls within the analytical concept of new wars or insecurity. Traditional wars also referred to as old wars were fought by regular armed forces of States for geopolitical interests or ideology where battle was the decisive encounter (Naughton, 2016) . New wars however, are the wars of the area of globalization and are fought by varying combinations of networks including State and non-state actors. There have been arguments that the next war to be fought is not likely to be traditional military war fare, but one fought in the cyber space by dismantling and disabling critical network infrastructures of other states – referred to as cyber warfare.

Therefore, this article is interested in examining the reasons that have informed cyber security policy formulation in Africa. It notes that Africa is one of the countries that have suffered most regarding cybercrime and yet a number of measures have been instituted by way of cyber legislations to avert such threats (Nir, 2019). I present a conceptual understanding of the concept of security and thus cyber security and its relationships to inform the arguments that indeed, policy making processes in Africa as far as cyber security is concerned has been crafted in ambiguity, completely overly exaggerated and hyper securitized without presenting specifications as to why certain issues become a security issue and others not. In fact, the conclusion is drawn that cyber security policy making in Africa is highly politicized to the level of threats politics. In order, to reach to these conclusions, fundamental questions are asked: what have influenced cyber security policy making in Africa? What are the referent objects of the State that are threatened and how do actors in security frame their threats? These questions may need to be interrogated beyond the mere every-day technical reasons advanced around vulnerabilities in networks and need to protect such systems. The paper notes that, it is quintessential that a deeper analysis of the processes that entails constructions of what is believed to be threatened by agents of security is crucial in unraveling the reasons and motives behind Africa Cyber security policy making.

2.0 Cyber Security and its origin

Discussing the origin of cyber security in the global North is essential in providing an historical trajectory of how insecurity logic was framed at that level and the extent to which such narratives became an organizing principle under which cyber security policy making in Africa were concluded. The information revolution sparked debates in the 1970s in the United States and built momentum in the 1980s and spread throughout other countries in the 1990s (Duun C. , 2007) . The debates were framed within the US Government circles and state bureaucracies, including military colleges, think-tanks, academia and the private sector that threats arising from digital technologies could have a devastating cascading consequence to society (Nissenbaum, 2009) . The need for protection of critical network infrastructures and other networks were deemed critical to secure the information networks and cyber space from actions of malevolent actors interested in causing mayhem and destruction by exploiting vulnerabilities in network systems.

At the continental level, fears of such vulnerabilities, the need to regulate the information society, fight cybercrime and balance competing interests in the digital space as far as safety and security is concerned prompted the African Union to adopt the AU Convention on Cyber Security and Personal Data Protection on the 27th of June 2014 which accordingly and in view of the mandate of the AU, African governments were not only expected to sign but also ratify the convention and streamline their cyber security laws within the framework of the AU convention.

At the East African level, the attack on the Kenyan Westgate Shopping Mall highlights the use of cyber space in planning, coordination, implementation and promotion of the various attacks and such attacks have destabilized and hampered recent economic growth performances. The Westgate Mall attack not only cost at least 67 innocent lives and millions of dollars in infrastructure damage, but it's also estimated to have cost the Kenyan economy $200 million in lost tourism revenue (UNECA, 2014). In Uganda, terrorist twin bombings during the world cup finals in Kampala claimed at least 74 lives with the Somali based Islamic militants – the Al-Shabab claiming responsibility of the attack (Rice, 2010) .

It is important to note that cyber security threats are often presented by policy makers, agents of security and even the mass media as one that is characterized by worst case scenarios. It is presented to look like it will come with substantial negative individual as well as societal consequences in the event information systems are infiltrated by malevolent actors and hence instilling fear and sense of urgency for authorities to work to address this impending and looming doom. However, the questions to reflect on are the seriousness of those threats in terms of its constitutive forms. In other words, insecurities have always existed and still do, and this paper by no means try to discredit that arrangement of things.

However, because of the urgency with which policy makers enact these laws and regulations its plausible to contend with the argument of (Duun C. , 2007) when she observes that cyber threats and insecurities are often shrouded in a cloud of speculative semantics worsened by definitions and ambiguous use of terminologies by many Government officials, which has created a tendency to hype the issue with rhetorical dramatization and alarmist warning (p.4). This is further compounded on by the work of news media that project worst case disaster scenarios and what the gloomy future is likely to be as a result of cyber insecurities and thus instilling fear among the masses. Furthermore, arguments have been advanced that combating cyber insecurities have not just become a highly politicized issue but also a lucrative one – indeed one where industries have emerged to grapple with the threats (Weimann, 2004a) and thus all these point to the competing interests that work at play to influence cyber security policy formulation in Africa.

In Uganda, actors of security do not clearly define what objects need to be protected or not and the normal function of State bureaucracies are always uncoordinated and yet not streamlined (Center, 2015). Besides, as a country there is no list of what is called critical national infrastructures and the lack of the list of what needs to be protected or not is mainly attributed to lack of knowledge and capacity on what particularly are critical network infrastructures (Center, 2015). Policy making in Africa often serves very broad and vague reasons ranging from issues such as fighting crime and preserving national security. Its also not surprising as reports show that most cyber security legislations in Africa especially countries such as Uganda, Tanzania and Kenya among others have been used to stifle internet rights, clamp down on rights activists or curtail views that are deemed to be critical of the State. There have been incidents where bloggers, journalists, and rights activists have been jailed and others disappeared in mysterious circumstances but also likely as a result of draconian cyber security policies that the State uses to curtail free speech and internet rights of its citizens (CIPESA, 2017) .

It is however, very important to note that there is a general consensus in the body of literature that points to the fact that whereas it appears that cyber security issues have been highly exaggerated and politicized in Africa as a result of manipulation, neither can it be denied that it doesn't exists nor should they be ignored (Denning, 2001b) mainly due to the unpredictable nature and speed of current and future technology development such as the 5th generation and Artificial Intelligence

3.0 Cyber Security threat framing

Cyber security has been framed in the context of Africa within three distinct levels that have informed and shaped the extent to which laws are crafted by most African governments. The distinct levels and the specific objects to be protected can be looked at as below:

a) **Technical discourse.** The idea that computer malwares – viruses, worms and trojans permeates through computer networks and infrastructures to cause damage and harm originates from this perspective. In other words, the securing of the cyber space from malevolent actors draws its inspiration from vulnerabilities associated with network computers and infrastructures that needs to be protected. This perspective is referred to as technification which draws its imperative from the speech acts of politicians and actor of security who uses technical languages to derive the need to secure networks and hence securitizing such from the technical point of view gives political actors credence to raise certain issues above politics (Buzan B. O., 1998) . Its in line with this reasoning that most States in Africa have drafted cyber security laws from the broad articulation of fighting crime and preserving national security due to vulnerabilities in the technical systems that can be manipulated by malevolent actors.

b) **Crime – espionage**. Cybercrime and espionage are also closely related to the technical discourse as crime takes place over computers and computer networks as referent objects. Financial fraud, espionage over businesses and private sector networks have been essential reasons advanced for the protection of the cyber space. Since States feel threatened, securitizing issues drawing from the need to protect the space from criminal elements as well as state sponsored cyber espionage topped the agenda of most of the countries in the global south.

d) The **military – civil defense.** This perspective is often drawn from the idea that the States have the legitimate responsibility over its territory and jurisdiction and thus must use the democratic legitimization that it has to defend the State from both offline and online actors. The idea of cyber warfare among States by way of intrusions into each other's critical network infrastructures shaped policy making processes in Africa as States looked to enact legislation that would criminalize activities of actors in the cyber space based on the principle of national security that always resonates well with them.

In line with the debates surrounding Cyber security and its evolution, cyber security policy formulation in Africa has tended to be reactionary, highly exaggerated as well as politicized and in part shaped by narratives that were carefully crafted in the global North about the devastating cyber disaster scenarios with large scale societal consequences. As (Duun C. , 2007) posits the Cyber security policy making in Africa was consequently influenced directly and indirectly by actions of other States that were able to extensively mobilize resources from within the different layers of State bureaucracies to shape threat perceptions and countermeasures associated in that regard but also more importantly influence from business actors inside and outside of States territorial jurisdiction and non-State actors that shaped threats and actions that States need to undertake to mitigate such threats.

It is important to note that nation states tend to exaggerate their security beyond the normal dangers of threats (Buzan B. O., 1998) . If this is the case, then could we conclude that many African States including the Ugandan State may have exaggerated their security fears based on risks and assumptions outside the normal reality of an existential threat which culminated into the enactment of various cyber security legislations within a short period of time? The concept of hyper-securitization is best suited to explain the arrangement of things within the context of cyber security policy making in Africa. (Buzan B. , 2004) defines cyber-security sector within the context of hyper-securitization referring it to the narrated, potential, future catastrophes of instantaneous, cascading destruction, coupled with the absence of historical incidents of the same magnitude (p.1163-5). The cascading nature of networked mega-catastrophes, coupled with the absence of such historical incidents, generates a strong urgency and drive to act upon a certain issue which the actors of security feels should be elevated above public policy or politics.

Security as a way of life produces different interpretations by different groups of people. For example, it has been argued that “different world views and discourses about politics deliver different views and discourses about security” (Booth, 1994) . If we are to follow the logic of such inquiry, then perhaps we need to understand how the arrangement of things played out in the context of countries such as Uganda. Certainly, (Booth, 1994) is suggesting that in security and threat framing many factors including politics, personal interest of the actors of security converges to influence and determine security issues. But beyond understanding and interrogating the aspects of national and cyber security policy, it’s not surprising to see how the rush in Uganda for example culminated in a series of legislations without the requisite competence to deal with threats for instance, reports suggest that Uganda still loses nearly 122 billion Uganda shillings on cyber-attacks annually despite the institutional mechanisms and legal frameworks established to avert the vice (Kamoga, 2017) . Certainly, a robust policy making processes that involves awareness raising, capacity building as well as participation from all actors – the broader stakeholder groups is essential, after all the legal frameworks alone is not enough to avert cybercrime or cyber insecurities.

Its thus important to note that (Buzan B. O., 1998) analysis supports the views of (Booth, 1994) when he argued that in security discourse “an issue is dramatized and presented as an issue of supreme priority; and thus labeling it as a security, an agent claims a need for and a right to treat it by extraordinary means and hence meaning that for an analyst or researcher to grasp the act, the task is not to assess some objective threats that really endanger some object to be defended or secured" but to clearly investigate and understand the processes that entail the construction of what is collectively believed to be a threat by the agents of security.

If establishing legal frameworks and intuitional mechanisms to fight cybercrimes was the epitome, the overarching, and overriding principle behind thwarting insecurity threats in the cyber space, then perhaps countries like Uganda would not be losing substantial amount of resources on fraudulent activities. This means, besides policy prescriptions other treatments such as capacity building, awareness raising, coordinated activities of government bureaucracies and private sectors among others is crucial in averting cyber insecurities. In other words, policy prescriptions as far as Cyber Security policy making in Africa is concerned has merely failed due to the absence of an analytical lense in security and threat framing and the lack of coordinated and well-streamlined institutional capabilities to contend with the phenomenon. Security is a way of life and involving the broader stakeholder groups by way of capacity building, awareness raising, enforcement of laws and legislative frameworks, societal culture just to mention but a few is instrumental in defining a secure cyber space for everyone. Undertaking policy formulation in exclusivity based on emotions, fears, risks and exaggerated assumptions impedes nation states' ability to objectively coordinate its efforts within its own layers of State bureaucracy, the private sector and even the broader stakeholder groups.

Uganda is one of the countries that in 2018 was ranked number one in Africa in terms of its cyber security readiness and yet at the moment the country does not have a list of Critical National Infrastructures and also the difficulty amongst its line institutions in the ICT sector in distinguishing what needs to be protected (Center, 2015) , the Ugandan Cyber security debate therefore, just like the rest of the continental Africa can rightly be argued to be highly politicized today suggesting that threats whether perceived or existential has been largely a matter of politicking in line with what (Duun C. M., 2012) calls "threat politics" – a political process that elevates threats above or out of politics.

4.0 Conclusion

This piece of work has rightly shown the historical roots around cyber security and how such framings were instrumental in shaping State behaviors especially in the global South regarding policing the cyber space. It also shows the three basic frameworks used to analyze cyber security policies and points out that the narrow understanding of those frames has perpetuated the illogical and blind cyber security policy making in Africa. The article delves into the literature and points out what the scholarships in the field of security shows regarding this phenomenon. I therefore, draw my conclusion based on the fact that security policy making in Africa in general is not based on construction of well-articulated threats because of the discursive interpretations of security that can be influenced by personal interests, fears, risks and assumptions by politicians and actors of security. Uganda and the rest of African Governments should reflect and rethink their security policy making processes, define referent objects of the State that needs to be protected and clearly articulate the processes that entails construction of what is believed to be a threat and more importantly, engage the broader stakeholder groups in such processes after all, security is a way of life that affects everyone including individuals, the State and the Society as a whole.

References

Baldwin, D. A. (1997). The Concept of Security. *Review of International Studies Vol. 23, no,1*, 5-26.

Booth, K. (1994). Security and Self: Reflections of a Fallen Realist. *York Center for International and Strategic Studies*.

Buzan, B. (2004). From international to world society? English school theory and the social structure of globalisation. *Cambridge Studies in International Relations Vol.1. 95*.

Buzan, B. O. (1998). Security: A New Framework for Analysis. *Boulder,CO: Lynne Rienner*.

Cabinet, O. (2011). *UK Cyber Security Strategy: Protecting and Promoting the UK in the Digital World.* London: Crown.

Center, G. C. (2015). Cyber Security Capacity Review of the Republic of Uganda.

CIPESA. (2017). The State of Internet Freedom in Africa.

Creasey, J. (2013). *Cyber Security Incident Response Guide.* Crest.

Denning, D. (2001b). Activism, Hacktivism and Cyber Terrorism: The Internet as a tool for influencing foreign policy. 239-288.

Duun, C. (2007). Cyber Security and Threat Politics.

Duun, C. M. (2012). Cyber Security and Threat Politics: US Efforts to Secure the Information Age. *Routledge*.

Kamoga, J. (2017). Uganda Loses Shs 122 bn Annually to Cyber Attacks, Says Report. *Retrieved July 1, 2019, from https://observer.ug/news/headlines/54458-uganda-loses-shs-122bn-annually-to-cyber-attacks-says-report.html*.

Naughton, J. (2016). The evolution of the internet: from military experiment to general purpose technology. *Journal of cyber policy*, 1:1, 5-28.

Nir, K. (2019). Cybercrime and Cyber Security in Africa. *Journal of Global Information Technology Management 22:2*, 77-81.

Nissenbaum, L. H. (2009). Digital Disaster, Cyber Security and the Copenhagen School. *International Studies Quarterly Vol.53.no.4*, 1155-1175.

Rice, X. (2010). Uganda Bomb Blasts Kills at least 74. *Retrieved July 1, 2019, from https://www.theguardian.com/world/2010/jul/12/uganda-kampala-bombs-explosions-attacks*.

Thierry Balzacq, M. D. (2016). A theory of actor-network for cyber-security. *European Journal of Internation Security Vol.1,no.2*, 176-198.

UNECA. (2014). Policy Brief: Tackling the Challenges of Cyber Security in Africa.

Weimann, G. (2004a). How Modern Terrorism Use the internet .